CLAIMS

1. (Previously presented) A method comprising:

requesting a service for a platform from a service provider;

receiving a service key request for the service from the service provider, wherein the service key is to be limited to one or more acceptable configurations of the platform;

generating a service key pair that is limited to the one or more acceptable configurations of the platform, and returning a public key of the key pair to the service provider;

certifying the use of the service for the one or more acceptable configurations of the platform; and

receiving a session key for a session of the service from the service provider, the service being limited to the one or more acceptable configurations of the platform.

2. (Previously presented) The method of claim 1, further comprising obtaining an identifying credential, wherein the identifying credential is provided to the service provider.

3. (Original) The method of claim 2, wherein the identifying credential comprises an attestation identification key (AIK) certificate.

4. (Original) The method of claim 2, wherein the identifying credential is obtained from a trusted third party.

PAGE 5/20 * RCVD AT 3/21/2008 8:40:22 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-4/3 * DNIS:2738300 * CSID:5033721083 * DURATION (mm-ss):05-54

5. (Original) The method of claim 2, wherein the identifying credential is obtained through a transaction with the service provider.

6. (Previously presented) The method of claim 1, wherein certifying the use of the service comprises includes a process selected from the group consisting of producing hash data relating to the one or more acceptable configurations; and confirming that a chosen configuration is included in a set of values representing the one or more acceptable configurations.

7. (Previously presented) The method of claim 1, wherein the service key is limited to platform configuration register values that represent the one or more acceptable platform configurations.

8. (Previously presented) A method comprising:

receiving a service request from a client for a platform;

creating a service key generation request for the client, wherein the service key is to be limited to one or more acceptable configurations of the platform;

receiving a public key of a service key pair from the client in response to the service generation request, the service key pair being limited to the one or more acceptable configurations of the platform;

validating the service key, validation of the service key comprising receipt of assurance that the service is used only for one or more acceptable configurations for the platform; and

PAGE 6/20 * RCVD AT 3/21/2008 8:40:22 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-4/3 * DNIS:2738300 * CSID:5033721083 * DURATION (mm-ss):05-54

providing a session key for the service to the client based on the validated service key, the service being limited to the one or more acceptable configurations.

9. (Original) The method of claim 8, further comprising receiving an identifying credential from the client.

10. (Original) The method of claim 9, wherein the identifying credential comprises an attestation identification key (AIK) certificate.

11. (Previously presented) The method of claim 8, wherein validating the service key comprises a process selected from the group consisting of sending a certification request to the client and receiving hash data relating to the one or more acceptable configurations; and sending a list of value sets for the one or more acceptable configurations to the client and receiving a confirmation that a chosen configuration is included in the list of value sets.

12. (Previously presented) The method of claim 8, further comprising limiting the service key to platform configuration register values that represent the one or more acceptable platform configurations.

13. (Previously presented) A client device comprising:

a communication device to communicate with a service provider, the client device to request a service from the service provider for a platform; and

a trusted platform module (TPM) to provide secure operations in connection with the service from the service provider;

PAGE 7/20 * RCVD AT 3/21/2008 8:40:22 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-4/3 * DNIS:2738300 * CSID:5033721083 * DURATION (mm-ss):05-54

wherein the client device is to:

receive a service key request for the service from the service provider, wherein the service key is to be limited to one or more acceptable configurations of the platform,

generate a service key pair that is limited to the one or more acceptable configurations of the platform and return a public key of the key pair to the service provider,

provide assurance to the service provider that the service is limited to the one or more acceptable configurations for the platform, and

receive a session key for a session of the service from the service provider, the service being limited to the one or more acceptable configurations of the platform.

14. (Original) The client device of claim 13, wherein the provision of assurance to the service provider comprises receiving a certification request from the service provider, producing hash data relating to the one or more acceptable configurations using the trusted platform module, and sending the hash data to the service provider.

15. (Original) The client device of claim 13, wherein the provision of assurance to the service provider comprises receiving a list of acceptable value sets relating to the one or more acceptable configurations and sending a confirmation that a chosen configuration is included in the list of acceptable value sets.

PAGE 8/20 * RCVD AT 3/21/2008 8:40:22 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-4/3 * DNIS:2738300 * CSID:5033721083 * DURATION (mm-ss):05-54

16. (Previously presented) A system comprising:

a client device, the client device comprising a trusted platform module, the client device to request a service for a platform of the client; and

a service provider to provide a service to the client device, the service provider to receive the service request from the client and create a service key generation request for the client, wherein the service key is to be limited to one or more acceptable configurations of the platform;

the client device to generate a service key pair in response that is limited to the one or more acceptable configurations of the platform and to return a public key of the key pair to the service provider, certify that the service will be utilized only in one or more acceptable configurations of a platform of the client device, and receive a session key for a session of the service from the service provider, the service being limited to the one or more acceptable configurations of the platform.

17. (Original) The system of claim 16, wherein the client device obtains an identifying credential.

18. (Original) The system of claim 17, wherein the identifying credential comprises an attestation identification key (AIK) certificate.

19. (Original) The system of claim 17, wherein the identifying credential is obtained from a trusted third party.

PAGE 9/20 * RCVD AT 3/21/2008 8:40:22 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-4/3 * DNIS:2738300 * CSID:5033721083 * DURATION (mm-ss):05-54

20. (Original) The system of claim 17, wherein the identifying credential is obtained through a transaction with the service provider.

21. (Previously presented) The system of claim 16, wherein certifying the use of the service comprises a process selected from the group consisting of producing hash data relating to the one or more acceptable configurations; and confirming that a chosen configuration is included in a set of values representing the one or more acceptable configurations.

22. (Previously presented) The system of claim 16, wherein the service key is limited to platform configuration register values that represent the one or more acceptable platform configurations.

23. (Previously presented) A computer-readable medium having stored thereon data representing sequences of instructions that, when executed by a processor, cause the processor to perform operations comprising:

requesting a service for a platform from a service provider;

receiving a service key request for the service from the service provider, where the service key is to be limited to one or more acceptable configurations of the platform;

generating a service key pair that is limited to the one or more acceptable configurations of the platform, and returning a public key of the key pair to the service provider;

certifying the use of the service for the one or more acceptable configurations of the platform; and

PAGE 10/20 * RCVD AT 3/21/2008 8:40:22 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-4/3 * DNIS:2738300 * CSID:5033721083 * DURATION (mm-ss):05-54

receiving a session key for a session of the service from the service provider, the service being limited to the one or more acceptable configurations of the platform.

24. (Original) The medium of claim 23, wherein certifying the use of the service comprises producing hash data relating to the one or more acceptable configurations.

25. (Previously presented) The medium of claim 23, wherein certifying the use of the service comprises confirming that a chosen configuration is included in a set of values representing the one or more acceptable configurations.

26. (Previously presented) A medium having stored thereon data representing sequences of instructions that, when executed by a processor, cause the processor to perform operations comprising:

receiving a service request from a client;

creating a service key generation request for the client, wherein the service key is to be limited to one or more acceptable configurations of the platform;

receiving a public key of a service key pair from the client, the service key pair being limited to the one or more acceptable configurations of the platform;

validating the service key, validation of the service key comprising receipt of assurance that the service is used only for one or more acceptable configurations; and

providing a session key for the service to client based on the validated key, the service being limited to the one or more acceptable configurations.

PAGE 11/20 * RCVD AT 3/21/2008 8:40:22 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-4/3 * DNIS:2738300 * CSID:5033721083 * DURATION (mm-ss):05-54

27. (Original) The medium of claim 26, wherein validating the service key comprises sending a certification request to the client and receiving hash data relating to the one or more acceptable configurations.

28. (Original) The medium of claim 27, wherein validating the service key comprises sending a list of value sets for the one or more acceptable configurations to the client and receiving a confirmation that a chosen configuration is included in the list of value sets.

PAGE 12/20 * RCVD AT 3/21/2008 8:40:22 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-4/3 * DNIS:2738300 * CSID:5033721083 * DURATION (mm-ss):05-54